



2023

Cisco Supplier Guide:

Sustainability, Risk, and Security



Table of Contents

- 01** Letter from John Kern
- 02** Using the Supplier Guide
- 03** Upholding Human Rights for All Supply Chain Workers
- 04** Acting on Climate Change and Our Environmental Stewardship
- 05** Promoting a Circular Economy
- 06** Ensuring Security
- 07** Providing Risk Management



Letter from John Kern



Dear Trusted Partners,

Cisco's supply chain is critical to its success, both as a public company and in its ability to make positive impacts on society and the planet. Cisco's partnerships with suppliers have led to a resilient, ethical and environmentally responsible supply chain. We have won awards and accolades, but we cannot rest on past achievements. We need to go further. We need to seize on shared opportunities around climate change, the circular economy and human rights to do great work, together.

In the following pages, you will read about the many ways we can collaborate to create positive impacts, including:

Acting on climate change: Cisco works with suppliers to set greenhouse gas (GHG) reduction goals and create systems that track progress on cutting emissions. Through ongoing dialogues, we listen to the problems our suppliers face, work with them to build greater capacity, and track hurdles to implementation.

Reimagining the lifecycle of Cisco products: Promoting a Circular Economy benefits both Cisco and our suppliers, with product design, sourcing, manufacturing and remanufacturing being key areas for collaboration. Consumers are demanding more socially responsible products and Cisco wants to work with suppliers who understand circular, rather than linear, thinking.

Upholding human rights for all supply chain workers: Supply chain workers are at the core of Cisco's human rights efforts, and the company does all it can to ensure people are treated equally and fairly. But we cannot do this alone. We need suppliers to help us prevent and remediate persistent problems such as forced and bonded labor, promote safe and healthy working conditions, and elevate workers' voices.

Suppliers help Cisco make our products, but they also act as stewards of the workforce and environments in which they operate. They are also on the front lines to make sure our collective networks stay safe and secure. Cisco sees this dynamic as a true partnership: working together we can solve large-scale problems and create positive impacts for our planet.

Sincerely,

John Kern

Senior Vice President, Cisco Global Supply Chain Operations



How to Use the Cisco Supplier Guide

The Cisco Supplier Guide highlights areas of importance around sustainability, risk, and security. This guide provides clarity on our specific reporting and compliance requirements and highlights areas that provide an opportunity to collaborate.

If you have any questions on any of the following guide categories, please email us at the following relevant email addresses:

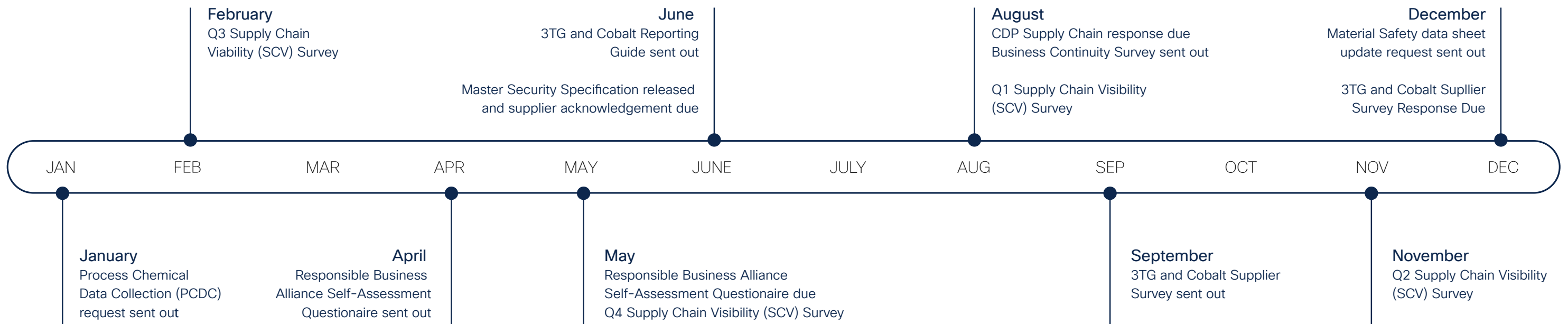
- Code of Conduct: cisco-supplier-coc@cisco.com
- Responsible Minerals: responsibleminerals@cisco.com
- Human Rights: humanrights@cisco.com
- Materials Compliance: supply_chain-cot_questions@cisco.com
- Circular Economy: circulareconomy@cisco.com
- Security: supply_chain_security@cisco.com
- Risk Management: supply-risk@cisco.com



As a Cisco supplier, you need to meet specific requirements by set deadlines. The following summarizes key deadlines you need to be aware of to stay in compliance with our Code of Conduct:

The contents of this guide are organized by topic, each with three detailed sections: *Why It Matters, Our Approach, and Supplier Expectations*. The Why It Matters section describes why Cisco cares about this topic. The Our Approach section details the actions Cisco takes to address this topic. The Supplier Expectations section outlines the actions suppliers must take to stay in compliance with Cisco’s Code of Conduct.

ANNUAL TIMELINE



RESPONSIBLE BUSINESS ALLIANCE (RBA) AUDIT PROCESS

Upholding Human Rights for All Supply Chain Workers

Supplier Code of Conduct and Human Rights

We are committed to manufacturing our products responsibly and sustainably. Cisco has a long-standing commitment to uphold and respect the human rights of all people, wherever we operate, including those who work in our supply chain. In our [Global Human Rights Policy](#), Cisco commits to upholding the human rights contained in the UN Universal Declaration of Human Rights and the International Labour Organization's eight Core Labour Conventions. Additionally, we adopt the three pillars set forth in the UN Guiding Principles on Business and Human Rights (UNGP).

Cisco uses the OECD Due Diligence Guidance for Responsible Business Conduct and the UN Guiding Principles for Business and Human Rights as the basis for our supply chain due diligence system. Establishing strong policies demonstrates our commitment, sets expectations for our suppliers, and helps guide how we and our suppliers operate. As a founding member of the Responsible Business Alliance (RBA), Cisco has adopted the RBA Code of Conduct ("the Code") as the [Cisco Supplier Code of Conduct](#). Cisco requires its suppliers to commit to abiding by the Code and ensure that these expectations are cascaded throughout the supply chain.

Why It Matters

Cisco seizes the opportunity and responsibility to leverage our business, global operations, and overall footprint to catalyze an inclusive future for all. Our Code plays a key role in this effort. By holding our suppliers accountable to the Code, we ensure consistent social and environmental responsibility standards are driven across the global supply chains. In addition to the Code, we expect our suppliers to abide by our [other responsible sourcing policies](#). These standards set a baseline from which to catalyze broad systems change.

Our Approach

In alignment with the UNGPs, Cisco uses a risk-driven approach when identifying suppliers in scope for human rights due diligence. To do this, Cisco engages suppliers to collect data to assess human rights risks, address and mitigate those risks, build capabilities, and prevent negative human rights impacts from occurring. Cisco also leverages RBA's tools, such as RBA audits to verify that suppliers adhere to the Code of Conduct.

We expect suppliers to adopt responsible business practices and governance structures consistent with the UNGP that promote respect for human rights. Suppliers must implement policies and processes to identify, prevent, mitigate, and remediate human rights impacts on the workers and vulnerable populations affected by their operations and supply chains. This includes adopting the RBA Code and cascading it to their suppliers. Moreover, suppliers should assist Cisco in meeting its objective of upholding human rights for those who work in our supply chain.

Cisco aims to drive continuous improvement and support the propagation of best practices throughout the supply chain. By collaborating with suppliers and peers, Cisco aims to develop solutions that are fit for their purpose and that can drive impact to measurably improve the lives of workers within the supply chain.

Supplier Expectations

Code of Conduct:

- Acknowledge and conform to the RBA Code of Conduct.
- Ensure that their suppliers are held accountable to the RBA Code of Conduct.
- Achieve and maintain consistent Code conformance aligned to at least RBA Silver Recognition.
- Share RBA Self-Assessment Questionnaires (SAQs) with Cisco and valid RBA Validated Assessment Program (VAP) audit reports through the RBA-Online platform. When requested by Cisco, perform RBA Customer-Managed Audits.
- Provide Corrective Action Plans for findings that occur through the audit process and close audit findings according to RBA closure guidelines.
- Maintain conformance to the Code after any audit findings are closed and as the Code is updated.

Cisco expects suppliers to be fully aware of, and be in conformance to, changes and updates to the RBA Code of Conduct. We also provide support to suppliers to achieve and maintain conformance to the Code, including capability building through e-learning courses, training sessions, or targeted coaching.

Please review the current Code at

www.responsiblebusiness.org/code-of-conduct/

Freely chosen employment and modern slavery:

- Maintain compliance and help Cisco to comply with relevant laws regarding forced labor due diligence and modern slavery disclosures.
- Cascade the RBA Code of Conduct standards on Freely Chosen Employment and [Definition of Fees](#) to their suppliers, recruitment agencies, and labor service providers. Additionally, conduct due diligence with recruitment agencies and labor service providers to ensure compliance.
- Protect workers, regardless of background, from [forced labor risks](#), such as those outlined by the International Labour Organization (ILO).

Young workers and child labor:

- Abide by the Cisco [Juvenile Labor Policy](#) for preventing child labor and protecting the rights of young workers, students, interns, and apprentices.

Health and safety and chemical management:

- Abide by the [Cisco Chemical Management Expectations](#) for Suppliers and RBA Process Chemicals Policy to protect workers and the environment from exposure to harmful chemicals.
- Adhere to the hierarchy of controls as a framework for protecting workers from workplace health and safety hazards and exposure to those hazards.
- Complete all the sheets contained in the [Process Chemical Data Collection \(PCDC\) Tool](#) and engage in deeper chemical exposure assessments when requested by Cisco.



For further questions or to get in touch, please email: humanrights@cisco.com

Responsible Minerals

Cisco has a long-standing commitment to promote responsible and ethical mineral procurement practices. The extraction and sale of certain minerals in conflict-affected and high-risk areas can be used to perpetuate violence, human rights abuses, environmental degradation, and other risks. Among the minerals of concern are tin, tungsten, tantalum, gold (3TG), and cobalt.

Why It Matters

Cisco does not directly procure minerals from mines, or from the smelters or refiners that process them. Therefore, we must work collaboratively through the supply chain to shift our mineral supply to responsible sources consistent with our values related to human rights, business ethics, labor, and environmental responsibility.

Our Approach

Cisco has implemented a comprehensive due diligence process to meet our regulatory obligations and to advance our goal of achieving a responsible mineral supply chain. Cisco participates in the Responsible Minerals Initiative (RMI) and leverages its tools and programs to conduct due diligence and advance responsible sourcing. These tools and programs include the Conflict Minerals Reporting Template (CMRT), Extended Minerals Reporting Template (EMRT), and Responsible Minerals Assurance Process (RMAP).

Supplier Expectations

We expect all suppliers to:

- Commit to the [Cisco Responsible Minerals Policy](#), which includes Cisco's expectations of suppliers regarding responsible sourcing of minerals.
- Maintain a policy and program for responsible mineral sourcing.
- Submit a CMRT or EMRT upon request from Cisco to document supply chain smelters used for products delivered to Cisco and verify key elements of the suppliers' policy and program.
- Source only from smelters validated as conformant with RMAP or a cross-recognized third-party assessment program.
- Create and share with Cisco plans for removing a smelter from its supply chain if sourcing from that smelter is identified by Cisco as high risk.



For further questions or to get in touch, please email: responsibleminerals@cisco.com

Acting on Climate Change and Our Environmental Stewardship

Cisco's owned and extended operations, including the manufacturing of our equipment, provide an important service in helping to power the Internet, but also require significant energy and natural resources. We have a responsibility to reduce the environmental impacts that result.

Why It Matters

To drive the large-scale change needed to decouple economic growth from environmental impact, it is important that we collaborate with our global network of component, manufacturing, and logistics suppliers, as well as our industry peers.

Our Approach

Environmental stewardship is a key consideration in our relationships with our suppliers. We reflect this by including sustainability requirements and performance in our supply chain business processes, educating stakeholders, and continually improving these processes. We evaluate our suppliers and help them drive improvement through leadership, support, and education.

To help us understand key impacts in our supply chain and how they are managed, we use recognized global frameworks and industry standards for accountability and reporting. We expect suppliers to publicly report GHG emissions, water use, and related reduction targets to CDP (formerly the Carbon Disclosure Project) on an annual basis. In addition, our Tier 1 suppliers are required to publish information in their annual reporting on the environmental impact of their operations and those of their suppliers, with the intent to continuously improve.

Supplier Expectations

We expect our suppliers to support Cisco in meeting our supply chain goals, as well as address material environmental impacts across their own operations and supply chain. Here is a summary of our goals:



*Excluding those contained in commodity components sourced from suppliers (e.g., plastic screws, fans, and cables).

**Goal validated by SBTi

GHG Emissions

Cisco has committed to achieve net zero GHG emissions by FY40, which includes our product use, operations, and supply chain. We have two interim goals on our path to a net zero supply chain:

- Have 80 percent of Cisco component, manufacturing, and logistics suppliers by spend put in place a public, absolute GHG emissions reduction target by FY25.
- Reduce supply-chain-related Scope 3 GHG emissions by 30 percent absolute by FY30

To support Cisco's journey to net zero, all first- and second-tier suppliers are expected to report GHG emissions and energy consumption to [CDP](#) on an annual basis. These requirements include:

- Providing a complete and accurate inventory of corporate-wide Scope 1 and 2 GHG emissions.
- Making the response publicly available via the option provided by CDP
- Demonstrating verification (third-party review) of reported GHG emissions
- Setting a public absolute GHG emissions reduction goal and publicly reporting annual progress against that goal
- Requesting that their own suppliers and business partners also report to CDP using the same process as above

Cisco has committed to science-based GHG targets. That means our goals align with what the latest climate science says is necessary to limit global warming to 1.5°C above preindustrial levels. We prefer that our suppliers' absolute GHG goals also align to an approved science-based methodology (1.5°C reduction scenario).

Water

We expect first- and second-tier suppliers to report water use and governance to CDP on an annual basis. These requirements include:

- Providing a complete and accurate corporate level water response for facilities worldwide
- Making the response publicly available via the option provided by CDP
- Setting a water-saving goal and reporting annual progress against that goal

Cisco also requests that select suppliers develop a water stewardship practice informed by the Alliance for [Water Stewardship \(AWS\) standard](#). This request applies to high-water-consuming suppliers located in high-water-stress areas.

Waste

Cisco has committed that 70 percent of Cisco component and manufacturing suppliers by spend will achieve a zero-waste diversion rate at one or more sites by FY25. To support Cisco in meeting this goal, first-tier manufacturing suppliers are expected to monitor and collect waste diversion data. These requirements include:

- Reporting facility-level data to Cisco as requested
- Striving to achieve a zero-waste diversion rate across each site

We have partnered with TRUE Zero Waste to improve reporting capabilities, provide training, and increase engagement throughout our supply chain. We encourage suppliers to seek third-party zero waste certification at their manufacturing sites.

Environmental Pollution

To supplement our core environmental work, Cisco engages with the [Institute of Public and Environmental Affairs \(IPE\)](#) to screen supplier sites based in mainland China for environmental violations or risks. We work with our suppliers to correct any environmental issues identified. Our areas of focus include wastewater, exhaust gas, and waste management and pollution mitigation, as well as tracking and addressing corrective action reports of illegal pollution. First- and second-tier suppliers based in mainland China are expected to:

- Register a company account on the IPE website and screen their legal company name in the pollution database.
- Identify any environmental violations, follow a process to manage those violations, and get delisted from the IPE pollution database within six months.

First-tier suppliers based in mainland China are also expected to:

- Request their next-tier suppliers with sites located in mainland China to also register in IPE.
- Screen next-tier suppliers' legal names in the IPE pollution database and send Cisco the screening results.
- Establish a process to manage their suppliers' environmental violations.



Materials Compliance

Cisco's Controlled Substance Specification (Cisco CSS-EDCS 661823 or Cisco CSS) establishes and communicates Cisco substance use, reporting, and documentation requirements to our suppliers and partners. The Cisco CSS (EDCS 661823) requires contract manufacturers, original design manufacturers (ODMs) and OEM suppliers, and component suppliers to be accountable to ensure that manufacturing consumables (bulk materials or process chemicals that are used to manufacture, assemble, or package products and that remain in the products) meet the requirements defined in the Cisco CSS.

Cisco requires suppliers and partners to:

- Acknowledge receipt of and comply with the Cisco CSS.
- Provide complete and accurate information to verify conformance when requested.

The Cisco CSS also references the requirements for packaging batteries or products that contain batteries. For packaging batteries or products that contain batteries, both the Cisco's Environmental Packaging Specification (EDCS 886022) and Cisco's Compliance Specification for Batteries and Products Containing Batteries (EDCS 627058) apply, respectively.

Public Reporting

First-tier suppliers are expected to:

- Publish a sustainability report based on the Global Reporting Initiative (GRI) Standards.
- Disclose supply chain environmental information in the GRI report, including:
 - Next-tier suppliers' environmental compliance information

For further questions or to get in touch, please email: supply_chain-cot_questions@cisco.com.



Promoting a Circular Economy

Cisco has changed the world many times over with our products. Now we're changing it again by transforming the way we do business—the way we design and build products and solutions, the way we think about the lifetime of an asset, and the way we use our technology to support customers in their own business transformations.

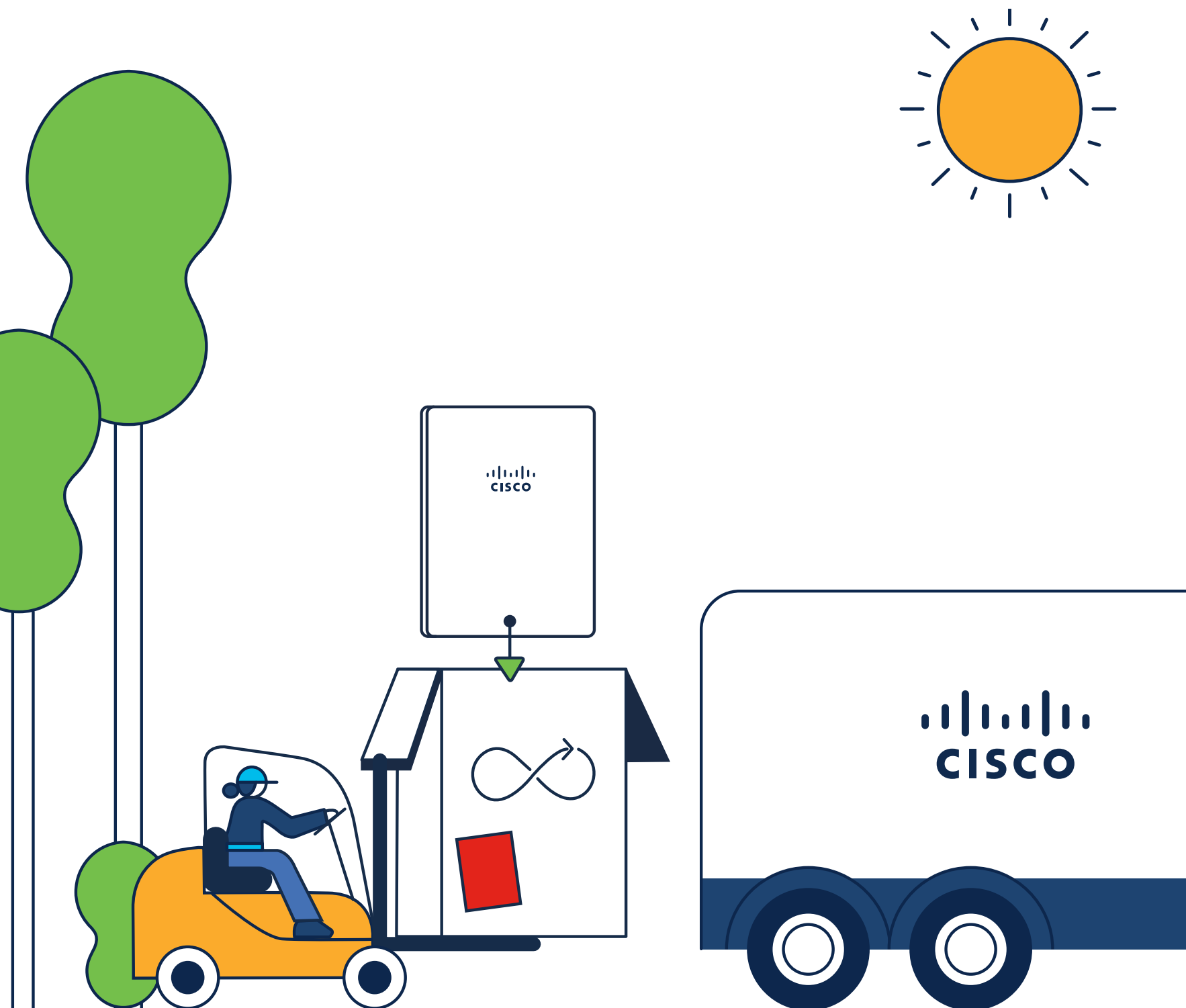
Why It Matters

Our commitment to a circular economy shows Cisco's proactive approach toward maximizing business continuity and resiliency in its supply chain while simultaneously adding value to our customers. Circularity also facilitates business operations that promote sustainability.

Our Approach

As part of Cisco's holistic approach to a circular economy, we aim for all of our resources to follow a circular model—where we reduce consumption, design out waste, and enable products and packaging to be used longer or reused. To achieve this, we are aligning our circular economy objectives with business operations and seeking out collaborative opportunities with suppliers. Suppliers are crucial in helping Cisco achieve the following commitments:





Supplier Expectations

Cisco asks all first-tier suppliers and strategic component and material suppliers to:

- Support Cisco's evolving circular economy objectives and related expectations of supplier.
- Evaluate packaging you use or provide to Cisco for opportunities to reduce overall packaging use, reduce packaging foam, eliminate plastic bags, and/or improve packaging efficiency.
- Respond promptly to all data requests (e.g., percent recycled content, component weight).

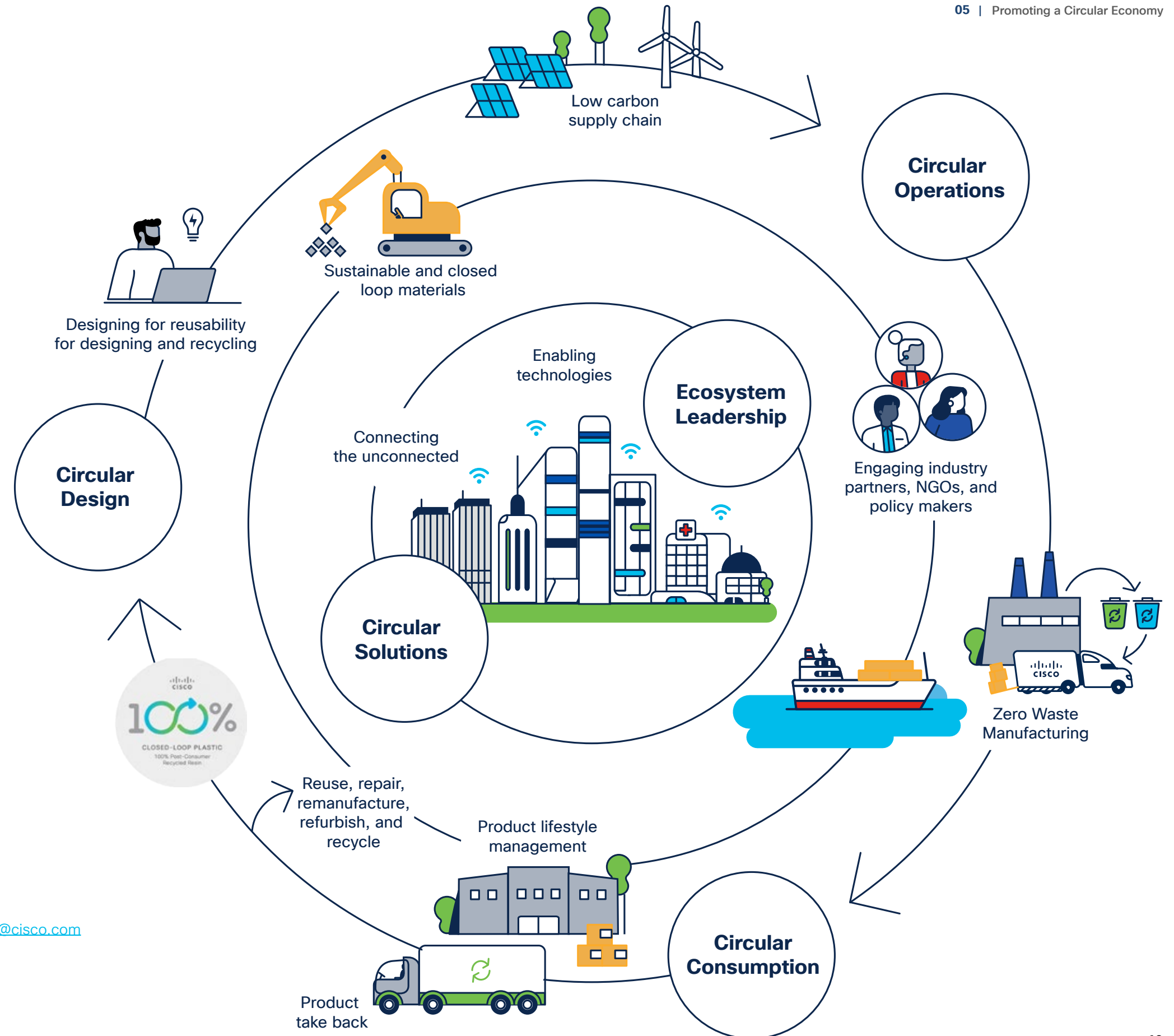
Cisco also asks all first-tier ODMs and Joint Design Manufacturers (JDMs) to:

- Review Cisco's ODM/JDM circular design playbook to understand and discuss expectations.
- Proactively work with Cisco design teams to evaluate product and packaging designs using the Cisco Circular Design Evaluation tool.
- Complete the Cisco Circular Design Questionnaire when requested.
- Incorporate necessary design changes into new products and packaging to meet circular design requirements.
- Share innovative ideas that will enhance circularity of Cisco products and packaging throughout lifecycle with Cisco product and packaging teams.

Please see the Climate Change and Environmental Stewardship section for more information on our work with suppliers to reduce our environmental impact, including GHG emissions, waste, and water.

The Cisco Circular Economy

A sustainable future is ours to create.



For further questions or to get in touch, please email: circulareconomy@cisco.com

Ensuring Security

Cisco drives security in our supply chain ecosystem to ensure that we can prevent and respond rapidly to any type of security threat. Our layered approach covers physical, logical, technical, and behavioral security.

Why It Matters

Security is an essential element of success to Cisco and our customers due to the pervasive impact of ever-evolving security threats. Threats have the potential to disrupt operations, result in financial losses, impact our brand reputation, and damage customer trust.

Our Approach

We are committed to enforcing security processes and practices to enable operational excellence and ensure brand protection and customers' trust. We are continuously strengthening our processes to protect Cisco intellectual property and prevent counterfeit or tainted products. Furthermore, we are striving to eliminate potential disruptions to supply chain services, such as sourcing, making, and delivery.

The Supply Chain Security team is responsible for overseeing the breadth of security issues across our supply chain. Cisco's supply chain is driving a comprehensive set of controls and measures to protect our products across our ecosystem.

To help Cisco Suppliers identify applicable security requirements, we communicate our Partner Requirements to our entire supply chain ecosystem through our Master Security Specification.

Cisco periodically monitors and measures our suppliers' compliance with all applicable requirements by using one or more of the following methods:

- Supplier audit performed by independent third parties
- Supplier audit performed by Cisco organizations, including, but not limited to, supply chain operations
- Supplier performance or business review
- Supplier evaluation upon contract renewal
- Supplier self-assessment
- Supplier security risk review prior to business award

For further questions or to get in touch, please email: supply_chain_security@cisco.com

Providing Risk Management

Our customers expect Cisco to deliver quality products and services on time, all the time. We want to continuously work side by side with our trusted Cisco suppliers and partners to prepare for unexpected events such as loss of critical assets, pandemic, technology outages, natural disasters, cyber threats, global environmental issues, and political instability by minimizing any downstream impact to our customers from these types of events.

Why It Matters

World-class risk management capabilities are driven through complete visibility of our supply chain locations and the appropriate levels of supplier and partner resiliency and preparedness in advance of a crisis. The impact of not being prepared is a risk to Cisco and could hinder our crisis response and ability to recover, which could then impact our commitments to our customers.

Our Approach

Our Business Continuity Plan (BCP) has a two-pronged approach. First, we aim to identify all supplier and partner site locations that manufacture parts for Cisco through Supply Chain Visibility (SCV). Second, we assess the risk of any of those sites being impacted by a global incident via a Supplier & Partner Business

Continuity Planning Assessment. To gather the supplier locations, our BCP team transmits a quarterly SCV survey to our suppliers via the Supplier Collection Form (SCF). In addition to sharing the locations (primary, subcontractor, and subtier) where they build Cisco parts, suppliers also need to provide the activities being performed for those parts and the associated total time to recover (TTR).

To assess the risk at the sites gathered in the SCV survey, the BCP team transmits the self-assessment BCP audit survey to our suppliers once every two years via the Supply Chain Content and Audit Management tool. The assessment includes documenting the supplier's recovery strategies and compliance to Cisco's supplier BCP standards, as well as identifying gaps in their BCP programs. Once the supplier completes the survey, the BCP team will review the responses and audit the evidence, until full compliance is achieved.

The BCP team works with our suppliers to mitigate and close any gaps by validating data through audits and drills. Global Supplier Management (GSM) Commodity teams are also available to assist suppliers with mitigation requirements. Additionally, Cisco senior management helps to review supplier BCP compliance status.

To ensure that we have the latest information at hand, Cisco requires continued support from suppliers. It's important that all survey requests from Cisco are treated with high priority in order to achieve complete visibility into our Tier 1 and Tier 2 supply network. This information enables faster identification of responsiveness to and recovery from any events that have the potential to disrupt Cisco business.

Supplier Expectations

For the SCV survey, suppliers will receive an email with the SCV attached. Suppliers need to respond with primary sites, subcontractor sites, sub-tier sites, activities, and TTR for Cisco parts and send the SCV survey back to scv-supply-risk@external.cisco.com before the deadline. For the BCP survey, suppliers need to log in to the Supply Chain Content and Audit Management tool, respond to the survey questions by site, and upload any necessary evidence in support of each survey question. Once completed, suppliers should submit the survey responses to Cisco for review.

Within 60 days following a request by Cisco, a supplier must respond in full to Cisco's questionnaire regarding disaster recovery, pandemic preparedness, and business continuity plans and measures specific to location(s) upon which the supplier relies on for providing the products. This information includes identifying primary site locations, available alternate facilities, time to recover (in weeks), emergency contacts, infrastructure and logistics, security, and protective measures necessary to ensure minimal impact to Cisco's supply of products.

Cisco may request an updated copy of such BCP periodically, but no more than biannually. An updated BCP provided by the supplier will supersede the prior BCP.



For further questions or to get in touch,
please email: supply-risk@cisco.com



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, see the Trademarks page on the Cisco website. Third-party trademarks mentioned are the property of their respective owners. The use of the word "partner" does not imply a partnership relationship between Cisco and any other company. (2204R)